UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,681	12/08/2003	Joon-Kit Goh	SE0039	5707

29393 7590 07/06/2007

ESCHWEILER & ASSOCIATES, LLC
NATIONAL CITY BANK BUILDING
629 EUCLID AVE., SUITE 1000
CLEVELAND, OH 44114

EXAMINER	
PATEL, NIRAV B	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
07/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/730,681	GOH, JOON-KIT	
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/21/04,12/08/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the application filed on 12/08/2003.

2. Claims 1-34 are under examination.

Specification

3. The disclosure is objected to because of the following informalities: The reference to application numbers provided in page 1 needs to be updated to reflect applications that have matured into patents. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claim 1-34 are rejected under 35 U.S.C. 102(e) as being anticipated Qi et al (US Patent No. 7,142,671).

As per claim 1, Qi discloses:

the DES engine having a message input, a cipher key input, and a pre-data output, the engine adapted to receive and selectively process a block of data from the message input of the security processing circuit during a first DES processing operation, and subsequently to process data from an intermediate result during second and third DES processing operations and store an intermediate result of the third DES processing operation to the pre-data output [Fig. 4A, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-14]; a security keys circuit having a set of cipher keys input and a key output, the security keys circuit operable to select and transfer a different cipher key to the key output coupled to the cipher key input of the DES engine selected from the set of cipher keys associated with each DES processing operation during the first, second and third DES processing operations [Fig. 4A – 419 col. 8 lines 29-64]; and a data output circuit having a pre-data input and a data output, the pre-data input of the data output circuit coupled to the pre-data output of the DES engine, and the data output selectively coupleable to the host system, the data output circuit operable to further security process data from the pre-data input and to selectively exclusive OR an initialization vector with the processed data and latch a final third DES result to the data output of the security processing circuit for use by the host system [Fig. 4A, 1, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-14].

As per claim 2, the rejection of claim 1 is incorporated and Qi discloses:

a permutation block PB having the message input and a permutation output, the permutation block PB operable to receive a block of data at the message input and to

perform an initial permutation of the message input data and provide a permutation result at the permutation output [Fig. 4A, 4B, 5, col. 7 lines 6-29, col. 9 lines 15-19];

a data input multiplexor DI Mux having a first and second input and a data selection output, the mux operable to select and couple one of the first and second inputs to the data selection output; an intermediate result register R_REG/L_REG having a data input, a clock input, and a latched data output, the register operable to store fight and left half results of the initial permutation or of a cipher process based on data present at the data input upon receipt of a clock signal at the clock input; eight cipher blocks having a data input, a key input, and a cipher output, operable to receive data at the data input and a key at the key input, to perform the cipher process comprising right and left halves of a sequential eight step cipher process on the data at the data input employing the key, and to provide a first and second cipher result during a first and second eight step cycle of each of the three DES processing operations[Fig. 4A, 4B, 5, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-32]; a pre-data output multiplexor PDO Mux having a first and second input and a data selection output, the mux operable to select and couple one of the first and second inputs to the data selection output [Fig. 4A,4B];and a pre-data output register PRE_DO having a data input, a clock input, and a latched data output [Fig. 4A, 4B], wherein the permutation output of the permutation block PB is coupled to the first input of the data input multiplexor DI Mux, the data selection output of the data input multiplexor DI Mux coupled to the data input of the intermediate result register R_REG/L_REG, the latched data output of the intermediate result register R_REG/L_REG coupled to the data input

of the eight cipher blocks having the cipher output of the eight cipher blocks feedback coupled to the second input of the data input multiplexor DI Mux and to the first input of the pre-data output multiplexor PDO Mux (81e) the data selection output of the pre-data output multiplexor PDO Mux coupled to the pre-data output register PRE_DO, the latched data output of the pre-data output register PRE_DO feedback coupled to the second input of the pre-data output multiplexor PDO Mux and the pre-data output [Fig. 4A, 4B, 5, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-32].

As per claim 3, the rejection of claim 2 is incorporated and Qi discloses:

wherein the DES engine is further operable to perform the initial permutation of the message input data using the permutation block PB, initially select the permutation result with the data input multiplexor DI Mux and couple and store the result to the intermediate result register R_REG/L_REG during a data input latch cycle, to transfer the initial result and the cipher key from the security keys circuit to the eight cipher blocks for cipher processing and intermediate storage of the right and left halves of the first eight step cipher results subsequent to selection of the second input of the data input multiplexor DI Mux into the intermediate result register R_REG/L_REG during the first cipher process cycle, to transfer the stored intermediate result and the cipher key from the security keys circuit to the eight cipher blocks for cipher processing and intermediate storage of the right and left halves of the second eight step cipher results subsequent to selection of the second input of the data input multiplexor DI Mux into the intermediate result register R_REG/L_REG and the pre-data output register PRE_DO

subsequent to selection of the first input of the pre-data output multiplexor PDO Mux during the second cipher process cycle of the first DES processing operation, and wherein the DES engine is operable to repeat the first and second cipher process cycles for the subsequent second and third DES security processing operations of the security processing circuit [Fig. 4A, 4B, 5, col. 7 lines 6-67-col. 8 lines 1-20, lines 44-67, col.9 lines 1-32], and latch the intermediate result of the third DES operation to the pre-data output of the pre-data output register PRE_DO of the DES engine, using the selection of the second input of the pre-data output multiplexor PDO Mux during the third DES processing operation of the 3DES security processing [Fig. 4A, 4B, col. 8 lines 44-67-col. 9 lines 1-14].

As per claim 4, the rejection of claim 3 is incorporated and Qi discloses:
wherein the 3DES processing is completed in three single DES processing operations [col. 5 lines 35-42, col. 8 lines 65-67].

As per claim 9, the rejection of claim 1 is incorporated and Qi discloses:
coupled to one or more of the DES engine, the security keys circuit, and the data output circuit for timing clock cycles of the first, second and third DES processing operations of the 3DES processing for the security processing circuit [Fig. 4A, 4B, 5].

As per claim 10, the rejection of claim 1 is incorporated and Qi discloses:

a set of cipher keys input, wherein the set of cipher keys comprise three different cipher keys, each cipher key associated with one of the three DES processing operations of the 3DES security processing [Fig. 4A]; a keys input multiplexor Key Mux having a set of cipher keys input, and a cipher key selection output, the mux operable to select and couple a cipher key to the cipher key selection output [Fig. 4A]; and a security keys register SK_REG having a data input, a clock input, and a latched data output, the register operable to store the cipher key selection associated with one of the three DES processing operations of the 3DES security processing based on cipher key data at the data input upon receipt of a clock signal at the clock input, the latched data output of the security keys register SK_REG coupled to the key input of the eight cipher blocks [Fig. 4A, col. 8 lines 29-67, col. 9 lines 1-14].

As per claim 11, the rejection of claim 10 is incorporated and Qi discloses:
the keys input multiplexor Key Mux is operable to receive the three cipher keys and to selectively couple one of the three cipher keys associated with a DES processing operation to the DES engine during the three DES processing operations of the 3DES security process [Fig. 4A].

As per claim 12, the rejection of claim 1 is incorporated and Qi discloses:
an inverse permutation block IPB having a pre-data input and an inverse permutation output, the block operable to receive and further security process the pre-data output from the DES engine, performing an inverse permutation of the pre-data

and transfer the processed data to the inverse permutation output [Fig. 4A, col. 9 lines 58-67, col. 10 lines 1-14];an XOR gate XOR having a processed data input, an initialization vector input, and an XOR gate output, the XOR gate operable to selectively exclusive OR the initialization vector at the initialization vector input together with the processed data from the inverse permutation output of the inverse permutation block coupled to the processed data input, and transfer the XOR data to the XOR gate output [Fig. 4A, 4B, col. 8 lines 44-64];a data output multiplexor DO Mux having a first and second input, a selection control signal, and a data selection output, the mux operable to select and couple one of the first and second inputs to the data selection output, based on the state of the selection control signal, the first input coupled to the XOR gate output, and the second input coupled to a data output register DO_REG [Fig. 4A, 4B]; and the data output register DO_REG having a data input, a clock input, and a latched data output, the register operable to store the output data results of the third DES process based on data present at the data input upon receipt of a clock Signal at the clock input, the latched data output of the data output register DO_REG feedback coupled to the second input of the data output multiplexor DO Mux to insure latching of the data at the output, wherein the data output circuit is operable to further security process data from the pre-data input and to selectively exclusive OR an initialization vector with the processed data and latch a final third DES result to the data output of the security processing circuit for use by the host system [Fig. 4A, 4B, 5, col. 8 lines 44-67, col. 9 lines 1-14].

As per claim 13, the rejection of claim 12 is incorporated and Qi discloses:

the data output circuit is operable to further security process data from the pre-data input and to selectively exclusive OR an initialization vector with the processed data and latch a final third DES result to the data output of the security processing circuit for use by the host system [Fig. 4A].

As per claim 14, the rejection of claim 1 is incorporated and Qi discloses:

wherein the security processing circuit resides within a network interface device of a host system for performing 3DES encryption and decryption services for the host system using a DES engine [Fig. 1, 4A, col. 3 lines 39-57].

As per claim 15, the rejection of claim 1 is incorporated and Qi discloses:

a network interface device coupled with the security processing circuit, the network interface device being adapted to selectively encrypt outgoing data from the host system to cryptographically process data for transmission to the network [Fig. 1, 4A, 4B].

As per claim 16, the rejection of claim 15 is incorporated and Qi discloses:

the network interface device comprises a bus interface, a media access control system, and the security processing circuit [Fig. 1].

As per claim 17, the rejection of claim 16 is incorporated and Qi discloses:

the network interface device is a single integrated circuit [Fig. 1].

As per claim 18, the rejection of claim 1 is incorporated and Qi discloses:
the circuit comprises an IPsec circuit adapted to selectively provide authentication, encryption, and decryption functions for incoming and outgoing data [Fig. 1, 2].

As per claim 19, it encompasses limitations that are similar to limitations of claim 2. Thus, it is rejected with the same rationale applied against claim 2 above.

As per claim 20, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 3. Thus, it is rejected with the same rationale applied against claim 3 above.

As per claim 21, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 4. Thus, it is rejected with the same rationale applied against claim 4 above.

As per claim 26, the rejection of claim 19 is incorporated and it encompasses limitations that are similar to limitations of claim 9. Thus, it is rejected with the same rationale applied against claim 9 above.

As per claim 27, Qi discloses:

selecting a permutation result of the initial permutation to couple the result to an intermediate result register during a first DES process; storing the permutation result in the intermediate result register [Fig. 4A col. 7 lines 12-61]; cipher processing the stored permutation result using an eight cipher blocks to generate an intermediate result of the cipher processing; selectively storing the intermediate result in the intermediate result register [Fig. 4A, 4B, 5, col. 8 lines 10-53]; cipher processing the stored intermediate result using the eight cipher blocks to generate a first DES result of the cipher processing [Fig. 4A, 4B col. 8 lines 44-67, col. 9 lines 1-14]; and selectively storing the first DES result in the intermediate result register [Fig. 4A, 4B].

As per claim 28, the rejection of claim 27 is incorporated and Qi discloses:
cipher processing the stored first DES result using the eight cipher blocks to generate a second intermediate result of the cipher processing [Fig. 4A, 4B, col. 8 lines 29-43]; selectively storing the second intermediate result in the intermediate result register [Fig. 4A, 4B]; cipher processing the stored second intermediate result using the eight cipher blocks to generate a second DES result of the cipher processing [Fig. 4A, 4B, col. 8 lines 29-43]; and selectively storing the second DES result in the intermediate result register [Fig. 4A, 4B, 5, col. 8 lines 44-67, col. 9 lines 1-14].

As per claim 29, the rejection of claim 28 is incorporated and Qi discloses:
cipher processing the stored second DES result using the eight cipher blocks to generate a third intermediate result of the cipher processing [Fig. 4A, 4B, col. 8 lines 29-

67, col. 9 liens 1-14]; selectively storing the third intermediate result in the intermediate result register [Fig. 4A]; cipher processing the stored third intermediate result using the eight cipher blocks to generate a third pre-data DES result of the cipher processing [Fig. 4A, 4B, col. 8 lines 44-67]; selectively storing the third pre-data DES result in the intermediate result register and selectively storing the third pre-data DES result in a pre-data output register [Fig. 4A, col. 8 lines 44-67]; performing an inverse permutation of the third pre-data DES result [Fig. 4A, col. 9 lines 34-65]; exclusively ORing the result of the inverse permutation with an initialization vector to generate a 3DES result [Fig. 4A, col. 8 lines 57-64]; and selectively latching the 3DES result to a data output register [Fig. 4A].

As per claim 30, Qi discloses:

receiving data of a permutation result of the initial permutation to a data input multiplexor during a first DES process [Fig. 4A col. 7 lines 12-61, 4B]; selecting and coupling the permutation result at the data input multiplexor to an intermediate result register; storing the permutation result in the intermediate result register[Fig. 4A, 4B]; transferring the stored permutation result and a cipher key to an eight cipher blocks for cipher processing; cipher processing using the eight cipher blocks to generate data of an intermediate result of the cipher processing [Fig. 4A, 4B, 5, col. 8 lines 10-53]; storing the intermediate result in the intermediate result register [Fig. 4A, 4B]; transferring the stored intermediate result and the cipher key to the eight cipher blocks for cipher processing [Fig. 4A, 4B]; cipher processing the intermediate result data using

the eight cipher blocks to generate a first DES result of the cipher processing [Fig. 4A, 4B]; and storing the first DES result in the intermediate result register [Fig. 4A, 4B].

As per claim 31, the rejection of claim 30 is incorporated and it encompasses limitations that are similar to limitations of claim 28. Thus, it is rejected with the same rationale applied against claim 28 above.

As per claim 32, the rejection of claim 31 is incorporated and it encompasses limitations that are similar to limitations of claim 29. Thus, it is rejected with the same rationale applied against claim 29 above.

As per claims 33 and 34, they encompass limitations that are similar to limitations of claim 30. Thus, they are rejected with the same rationale applied against claim 30 above.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Graunke et al (US 6947558) – Stream cipher having a shuffle network combiner function

Butter et al (US 5381480) --- System for translating encrypted data

Tham et al (US 2002/0061107) --- Methods and apparatus for implementing a cryptography engine

Matsuzaki et al (US 5,351,299) --- Apparatus and method for data encryption with block selection keys and data encryption keys

Buer (US 5671284) --- Data encryptor having a scalable clock

Anand (US 2003/0002664) --- Data encryption and decryption system and method using merged ciphers

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NBP
6/21/07

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100